ABSTRACT OF THE DISCLOSURE

An encryption apparatus provided with a Feistel type encryption algorithm includes a function operation unit that operates a non-linear function, and changing unit configured to supply the function operation unit with random data unrelated to an encryption operation result. In this way, a countermeasure can be taken against a DPA attack following the end of an operation by the encryption operation apparatus provided with the Feistel type encryption algorithm.